US 20170063540A1

(19) United States

(12) Patent Application Publication

Blommaert et al.

(10) Pub. No.: US 2017/0063540 A1

(43) Pub. Date: Mar. 2, 2017

(54) SECURE BOOTSTRAPPING ARCHITECTURE METHOD BASED ON PASSWORD-BASED DIGEST AUTHENTICATION

(71) Applicant: **Nokia Solutions and Networks Oy**, Espoo (FI)

(72) Inventors: **Marc Blommaert**, Elversele (BE); **Guenther Horn**, Munchen (DE)

(73) Assignee: **Nokia Solutions and Networks Oy**

(21) Appl. No.: **15/347,156**

(22) Filed: **Nov. 9, 2016**

Related U.S. Application Data

(63) Continuation of application No. 12/918,856, filed on Feb. 28, 2011, now Pat. No. 9,526,003, filed as application No. PCT/EP2008/001479 on Feb. 25, 2008.

Publication Classification

(51) **Int. Cl.**

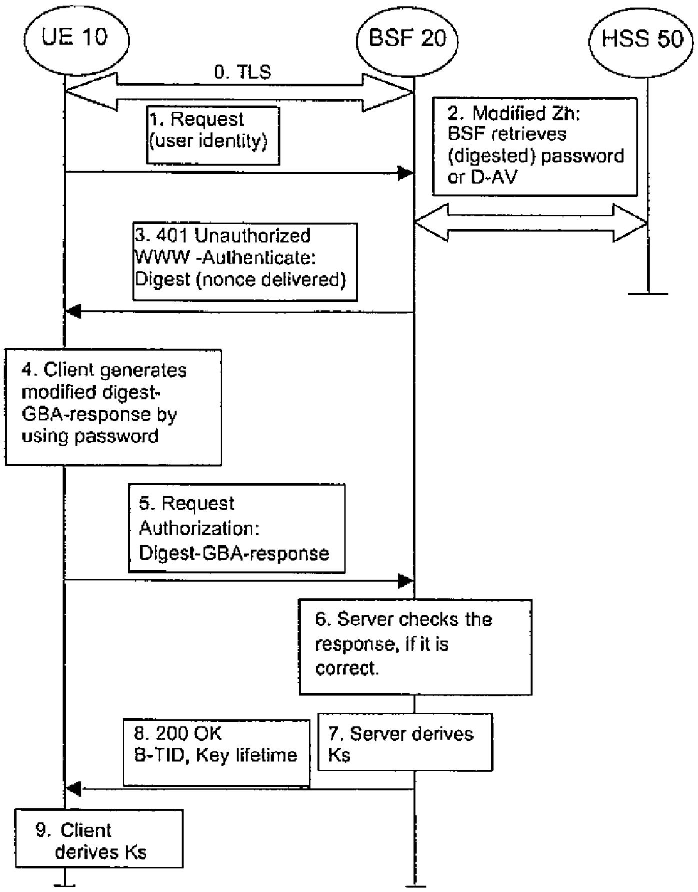
H04L 9/08	(2006.01)
H04W 12/06	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 9/0819*** (2013.01); ***H04L 9/0863*** (2013.01); ***H04L 9/0869*** (2013.01); ***H04W 12/06*** (2013.01); *H04L 67/02* (2013.01)

(57) ABSTRACT

A method, apparatus, and computer program product, in which a password-based digest access authentication procedure is used for performing authentication between a client and a server, wherein the authentication procedure is secured by at least one of modifying a digest-response parameter with a user password and generating a bootstrapped key based on the user password and at least one fresh parameter not used in a previous protocol run between the client and the server.


UE 10
BSF 20
HSS 50
0. TLS
1. Request (user identity)
2. Modified Zh: BSF retrieves (digested) password or D-AV
3. 401 Unauthorized WWW -Authenticate: Digest (nonce delivered)
4. Client generates modified digest-GBA-response by using password
5. Request Authorization: Digest-GBA-response
6. Server checks the response, if it is correct.
7. Server derives Ks
8. 200 OK B-TID, Key lifetime
9. Client derives Ks